# Generatory i odwrotność multiplikatywna modulo

**Treść:** Napisać program, który wyszukuje wszystkie generatory ciała Zp oraz program, który wylicza odwrotność multiplikatywną w Zp oraz Zn (pamiętaj o obsłudze przypadków, gdy odwrotność nie istnieje; n jest iloczynem dwóch liczb pierwszych).

**Rozwiązanie:**

Wyszukiwanie wszystkich generatorów ciała – działa na bazie liczności grup cyklicznych kolejnych elementów.

Obliczanie odwrotności multiplikatywnej w - działa na podstawie wzoru:

# Mnożenie i dzielenie wielomianów

**Treść:** Napisz program realizujący mnożenie i dzielenie wielomianów nad GF(p) dla dowolnego p. Sprawdź jego działanie dla ciała o charakterystyce innej niż 2.

**Rozwiązanie:** Stworzyłem klasę ExtendedModular, która reprezentuje element ciała rozszerzonego. Po tej klasie dziedziczy PolynomialModular, która jest reprezentacją wielomianową elementu ciała rozszerzonego. W tej klasie też zaimplementowałem dodawanie, odejmowanie, mnożenie i dzielenie wielomianów nad ciałami rozszerzonymi.

# Wyszukiwanie wielomianów nierozkładalnych

**Treść:** Napisz program, który wyszukuje wszystkie wielomiany nierozkładalne stopnia m nad ciałem GF(p).

**Rozwiązanie:** Cytując za artykułem z zajęć:

*„Niech będzie liczbą naturalną i będzie wielomianem dodatniego stopnia o współczynnikach całkowitych należących do zbioru . Jeśli jest liczbą pierwszą, to wielomian jest nierozkładalny nad .”*

Aby znaleźć wszystkie wielomiany stopnia nad ciałem wystarczy wygenerować wszystkie -elementowe wariacje liczb z , a następnie usunąć wariację zerową oraz te, które nie mają na najstarszej pozycji niezerowego elementu. Z tej listy wariacji (które mogą być traktowane jako wektory współczynników wielomianów) te reprezentują wielomiany nierozkładalne, dla których powyżej zacytowane twierdzenie jest prawdziwe.

# Reprezentacja elementów w ciałach rozszerzonych

**Treść:** Znajdź sposoby reprezentacji elementów ciała oraz metody wygenerowania tych reprezentacji. Ile jest reprezentacji, czym się różnią a w czym są podobne? Wygeneruj przynajmniej dwie reprezentacje elementów ciała dla jednej z par <p=2, m=5>, <p=3,m=3> albo <p=5, m=2>.

**Rozwiązanie:**

Elementy ciał rozszerzonych mogą być reprezentowane w różnoraki sposób, w zależności od tego jakie działania będą na nich wykonywane.

1. Potęga całkowita elementu abstrakcyjnego , a więc kolejne elementy ciała to: .
   * Mnożenie:
   * Dodawanie:

W celu umożliwienia dodawania można skorzystać z logarytmu Zecha:

(tylko w

Np.: :

Do powyższej zależności nie da się zastosować logarytmu Zecha, należy ją wpierw odpowiednio przekształcić:

A więc: , .

* + Generowanie:

Generowanie polega na wypisaniu wszystkich niezerowych elementów z ich potęgami.

1. Reprezentacja wektorowa – element ciała przedstawiany jest za pomocą wektorów o współczynnikach z . Jeśli jest generatorem ciała rozszerzonego, to istnieje taka, że .
   * Dodawanie:

Dodawanie uzyskuje się poprzez dodawanie współczynników wektora.

* + Mnożenie:

Potrzebna jest tabliczka mnożenia dla:

* + Generowanie:

Elementy można otrzymać na podstawie sekwencji pseudolosowej generowanej przez wielomian pierwotny służący do konstrukcji ciała rozszerzonego. Aby wygenerować sekwencję pseudolosową należy napisać zależność rekurencyjną stowarzyszoną z wielomianem pierwotnym. Np.:

,

Zadając ciąg początkowy otrzymana sekwencja losowa wygląda następująco:

Kolejne elementy otrzymuje się poprzez przesuwanie -elementowego okna nad powyższą sekwencją pseudolosową otrzymamy kolejne elementy ciała .

Tylko wielomiany pierwotne generują sekwencje pseudolosowe o okresie równym .

1. Reprezentacja wielomianowa – elementy reprezentowane są poprzez wielomiany, uzyskiwane jako reszta z dzielenia elementu w postaci potęgowej przez generator.

Np.: dla z generatorem element można przedstawić następująco:

Kolejne elementy można uzyskiwać poprzez mnożenie, np.:

* + Dodawanie:

Uzyskiwane poprzez dodawanie wielomianów.

* + Mnożenie:

Uzyskiwane poprzez mnożenie wielomianów.

1. Reprezentacja macierzowa

# Literatura

# Bibliografia

Andrzej Nowicki, A. Ś. (1997, wrzesień 30). Wielomiany nierozkładalne i liczby pierwsze. Toruń.

Mochnacki, W. (2000). *KODY KOREKCYJNE I KRYPTOGRAFIA.* Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej.